BEST AVAILABLE IMAGES

Defective images within this document are accurate representation of The original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : **H04M 1/274, G06F 1/00** — **A1**

(11) Numéro de publication internationale: **WO 98/13984**

(43) Date de publication internationale: 2 avril 1998 (02.04.98)

(21) Numéro de la demande internationale: PCT/FR97/01685

(22) Date de dépôt international: 25 septembre 1997 (25.09.97)

(30) Données relatives à la priorité:
96/11912 25 septembre 1996 (25.09.96) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: FINTEL S.A. [FR/FR]; 87, boulevard Haussmann, F-75008 Paris (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: ROSSET, Franck [FR/FR]; 96, boulevard Beaumarchais, F-75011 Paris (FR). GAYET, Alain [FR/FR]; 13, place des Dominos, F-92400 Courbevoie (FR). MOULIN, Jean [FR/FR]; 5, avenue de Beauséjour, F-92210 Draveil (FR).

(74) Mandataire: VIDON, Patrice; Cabinet Patrice Vidon, Immeuble Germanium, 80, avenue des Buttes de Coësmes, F-35700 Rennes (FR).

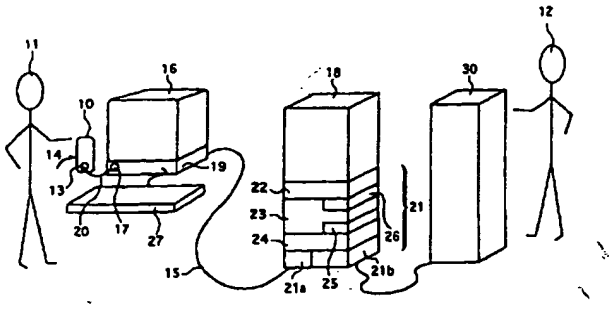
(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, brevet ARIPO (GH, KE, LS, MW, SD, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si de telles modifications sont reçues.

(54) Title: METHOD AND SYSTEM FOR ENSURING THE SECURITY OF SERVICE SUPPLIES BROADCAST ON A COMPUTER NETWORK OF THE INTERNET TYPE

(54) Titre: PROCEDE ET SYSTEME POUR SECURISER LES PRESTATIONS DE SERVICE DIFFUSEES SUR UN RESEAU INFORMATIQUE DU TYPE INTERNET

(57) Abstract



The invention concerns a method and a system enabling users (11) of an Internet type computer network provided with multimedia terminals (16) comprising a microphone (17) and connected to an Internet type computer network (15), remotely located from a service supplier (12), to accede rapidly and safely, to services (30) offered by this service supplier (12). The method comprises the following steps: the service supplier (12) provides each of the users (11) of an Internet type computer network (15) who have subscribed to his services (30), a card, formatted like a credit card; said card (10), formatted like a credit card, emits brief identifying sound signals (20), of the DTMF type, at least partly encrypted, varying with each operation, when it is actuated (14) by the user (11); said identifying sound signals are received by the microphone (17) of the multimedia terminal (16) and transmitted via the Internet type computer network (15) to the computer service (18) of the service supplier; the transmitted signals and the identification data of the subscriber and the card in the possession (23) of the computer service (18) are electronically processed (24) and compared (25) by the computer service. In the event of coincidence, the subscriber is immediately put through to the services (30) of the service supplier (12).

(57) Abrégé

L'invention concerne un procédé et un système permettant aux utilisateurs (11) d'un réseau informatique du type Internet disposant de terminaux multimédia (16) comportant un microphone (17) et connectés à un réseau informatique du type Internet (15), situés à distance d'un prestataire de service (12), d'accéder de manière sûre et rapide, aux services (30) offerts par ce prestataire de service (12). Le procédé comprend les étapes suivantes: le prestataire de service (12) met à la disposition de chacun des utilisateurs (11) d'un réseau informatique du type Internet (15) qui se sont abonnés à ses services (30), une carte (10), au format carte de crédit; ladite carte (10), au format carte de crédit, émet de brefs signaux acoustiques d'identification (20), de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée (14) par l'utilisateur (11); lesdits signaux acoustiques d'identification sont reçus par le microphone (17) du terminal multimédia (16) et transmis via le réseau informatique (15) du type Internet au service informatique (18) du prestataire de service; les signaux transmis et les données d'identification de l'abonné et de la carte détenues (23) par le service informatique (18) sont traités (24) et comparés (25) électroniquement par le service informatique (18) du prestataire de service. En cas de coïncidence, l'abonné est immédiatement mis en communication avec les services (30) du prestataire de service (12).

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

Procédé et système pour sécuriser les prestations de service diffusées sur un réseau informatique du type Internet

Le domaine de l'invention est celui de la transmission de données sur un réseau informatique du type Internet.

Plus précisément, l'invention concerne un procédé et un système permettant aux utilisateurs d'un réseau informatique du type Internet disposant de terminaux multimédia comportant un microphone et connectés à un réseau informatique du type Internet, situés à distance d'un prestataire de service, d'accéder de manière sûre et rapide, aux services que ce prestataire de service offre à ses abonnés au moyen d'un réseau informatique du type Internet.

Le problème posé est d'empêcher un utilisateur mal intentionné d'accéder aux services offerts par les prestataires de service sans y être autorisé, sans acquitter les droits correspondants ou en prétendant qu'il n'a pas demandé les services qui lui sont débités.

Pour résoudre ce problème, il a été proposé d'utiliser des clés d'accès que l'utilisateur génère au moyen de son terminal multimédia ou au moyen d'équipements périphériques. Ces solutions, outre leur coût, sont peu pratiques et longues à mettre en oeuvre. En fait, le problème posé ne peut être effectivement résolu que si on sait résoudre simultanément un autre problème : concevoir un procédé et un système commode d'utilisation, rapide à mettre en oeuvre en oeuvre et économique. En effet, dès lors que l'on s'adresse à un large public, la facilité d'utilisation et les gains de temps deviennent des problèmes majeurs qui ne peuvent pas être écartés.

Il a été proposé (document WO 96 04741 au nom de Andrew MARK) d'utiliser une carte émettant des signaux acoustiques, cryptés, de type DTMF, pour composer des numéros téléphoniques. Ainsi, le porteur d'une telle carte, en accouplant celle-ci au microphone du combiné téléphonique, transfert automatiquement ses identifiants. Comme ces identifiants sont chiffrés, on peut penser qu'un tiers ne sera pas en mesure d'en comprendre le contenu.

La solution de A. MARK, concerne donc un tout autre secteur technique que celui de la sécurité des données transmises sur un réseau informatique du type Internet. Au surplus, l'enregistrement des signaux émis par la carte A. MARK reste possible et un fraudeur

muni d'un tel enregistrement peut se substituer au bénéficiaire de la carte. La carte A. MARK ne permettrait donc pas d'empêcher un utilisateur mal intentionné d'accéder, sans y être autorisé, aux services offerts sur les réseaux informatiques du type Internet.

Les objectifs visés par la présente invention sont atteints et les problèmes que posent les techniques selon l'art antérieur sont résolus, selon l'invention, à l'aide du procédé suivant :

- le prestataire de service met à la disposition de chacun des utilisateurs d'un réseau informatique du type Internet qui se sont abonnés à ses services, une carte, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque abonné et pour chaque carte, la dite carte, au format carte de crédit, émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée par l'utilisateur d'un réseau informatique du type Internet,
- les dits signaux acoustiques d'identification sont reçus par le microphone du terminal multimédia et transmis via le réseau informatique du type Internet au service informatique du prestataire de service, notamment après réception par le terminal multimédia d'un ordre de transmission émis par le service informatique,
- les signaux transmis et les données d'identification du client et de la carte détenues par le service informatique sont traités et comparés électroniquement par le service informatique du prestataire de service,

de sorte qu'en cas de coïncidence l'abonné est immédiatement mis en communication avec le serveur informatique du prestataire de service.

Ainsi, grâce à ce procédé, le prestataire de service a l'assurance que l'appelant dispose bien d'une carte authentique et non d'un leurre informatique. Il a pu également identifier le titulaire de la carte comme étant une personne habilitée à utiliser les services qu'il offre.

Par ailleurs, les fraudeurs n'ont pas la possibilité de dérober les données d'identification puisque celles-ci sont transmises automatiquement sous une forme cryptée. En outre, l'enregistrement, sous quelque forme que ce soit, des signaux acoustiques ne sera d'aucune utilité à un fraudeur pour se faire identifier par les services informatiques du prestataire de service. En effet, les signaux acoustiques d'identification varient à chaque opération. C'est à dire chaque fois que la carte est actionnée.

De préférence la dite carte :

- décompte en outre le nombre de fois C(p,n) où elle est actionnée,
- émet des signaux acoustiques représentatifs du nombre de fois C(p,n) où elle a été actionnée,
- crypte les signaux acoustiques en fonction du nombre de fois C(p,n) où elle a été actionnée.

De préférence également, les dits moyens informatiques pour traiter et comparer électroniquement les signaux transmis et les données d'identification du client et de la carte détenues par le service informatique du prestataire de service :

- mémorisent le nombre de fois C(p,m) où la carte a été actionnée lors de la dernière opération validée,
- comparent le nombre de fois C(p,n) où la carte a été actionnée, lors de l'opération en cours, avec le nombre de fois mémorisé N1,
- rejettent l'opération en cours si C(p,n) est inférieur ou égal à C(p,m) et poursuivent la vérification de l'opération en cours si C(p,n) est supérieur à C(p,m),
- recalculent les signaux électroniques S'(p,n) en fonction des données d'identification et du nombre de fois C(p,n) où la carte a été actionnée, lors de l'opération en cours, puis les comparent aux signaux électroniques S(p,n) transmis. De sorte qu'en cas de coïncidence, l'utilisateur abonné peut être immédiatement mis en communication avec les services du prestataire de service.

Afin d'augmenter la sécurité du procédé, dans une variante de réalisation, le procédé comprend en outre l'étape suivante : l'abonné émet, au moyen d'un clavier associé au terminal multimédia et/ou à la carte, un code confidentiel. Après transmission au service informatique du prestataire de service, via le réseau informatique de communication, ce code confidentiel est traité et comparé au code confidentiel personnel de l'abonné détenu par le service informatique du prestataire de service.

Ainsi, le prestataire de service a l'assurance que l'appelant est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

Dans une autre variante de réalisation, afin également de renforcer la sécurité du procédé

et d'éviter que l'abonné ne puisse contester la demande qu'il a adressée au prestataire de service, le procédé comprend en outre les étapes suivantes :

- les ordres donnés par l'abonné au prestataire de service sont validés par l'abonné en actionnant la carte pour qu'elle émette un signal acoustique crypté de validation,
- le dit signal de validation est enregistré par le service informatique du prestataire de service, traité et décrypté, et de préférence un accusé de réception est adressé à l'abonné.

Grâce à ce procédé, l'abonné a validé, par une signature électronique, l'ordre qu'il a donné au prestataire de service.

Au moins trois variantes de réalisation permettent de transmettre les signaux acoustiques d'identification au service informatique du prestataire de service.

Selon la première variante, le procédé selon l'invention comprend en outre les étapes suivantes :

- le service informatique du prestataire de service télécharge dans le terminal multimédia un logiciel de conversion,
- le logiciel de conversion convertit, sous la forme d'une séquence de bits, les signaux acoustiques d'identification reçus par le microphone du terminal multimédia,
- la séquence de bits est transmise, via le réseau informatique du type Internet, au service informatique du prestataire de service, notamment après réception d'un ordre de transmission émis par le service informatique.

De sorte que les signaux provenant du terminal multimédia se présentent sous la forme d'une séquence de bits.

Selon la deuxième variante de réalisation, les signaux acoustiques d'identification reçus par le microphone du terminal multimédia sont transmis via le réseau informatique du type Internet au service informatique du prestataire de service, notamment après réception par le terminal multimédia d'un ordre de transmission émis par le service informatique. Dans le cas de cette variante, les signaux provenant du terminal multimédia sont transmis sous la forme d'un fichier son. Le traitement du fichier son et sa transformation en une séquence de bits (éléments binaires) sont effectués par les services informatiques du prestataire de service.

Selon la troisième variante le procédé comprend en outre les étapes suivantes :

- le prestataire de service met à la disposition de chacun des utilisateurs du réseau informatique du type Internet qui se sont abonnés à ses services, un logiciel de conversion destiné à être mis en oeuvre dans le terminal multimédia,
- les dits signaux acoustiques d'identification reçus par le microphone du terminal multimédia sont convertis en séquence de bits, avant d'être transmis via le réseau informatique du type Internet au service informatique du prestataire de service.

L'invention concerne également un système permettant aux utilisateurs du réseau informatique du type Internet disposant de terminaux multimédia comportant un microphone et connectés à un réseau informatique du type Internet, situés à distance d'un prestataire de service, d'accéder de manière sûre et rapide aux services que le dit prestataire de service offre aux utilisateurs. Ce système a pour caractéristique de comprendre les moyens de mise en oeuvre du procédé ci-dessus défini et de ses variantes de réalisation.

Plus particulièrement :

- Le système selon l'invention comprend une carte, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et pour chaque abonné, mise à la disposition de ceux-ci. La dite carte comporte:
  * des moyens d'émission de brefs signaux d'identification, de type DTMF, actionnés par l'abonné au moyen d'un élément accessible de l'extérieur de la carte,
  * des moyens de cryptage permettant de crypter au moins en partie et de varier les signaux acoustiques chaque fois que la carte est actionnée.
- Le système selon l'invention comprend des moyens de transmission des signaux acoustiques, situés dans les terminaux multimédia, transmettant à distance sous la forme de signaux électroniques, via le réseau informatique du type Internet, les dits signaux acoustiques.
- Le système selon l'invention comprend des moyens informatiques, dépendants des services informatiques du prestataire de service, connectés au réseau informatique du type Internet et recevant les signaux électroniques provenant des terminaux multimédia. Les moyens informatiques comprennent :
  * une base de données contenant les références des cartes et des abonnés et leurs

données d'identification,

* des moyens de traitement et des moyens de comparaison des signaux électroniques et des données d'identification contenues dans la base de données.

De sorte qu'en cas de coïncidence les services du prestataire de service sont immédiatement accessibles aux abonnés.

Ainsi, grâce à ce système, le prestataire de service a l'assurance que l'appelant dispose bien d'une carte authentique et non d'un leurre informatique. Il a pu également identifier le titulaire de la carte comme étant une personne habilitée à utiliser les services qu'il offre. Par ailleurs, les fraudeurs n'ont pas la possibilité de dérober les données d'identification puisque celles-ci sont transmises automatiquement sous une forme cryptée. En outre, l'enregistrement, sous quelque forme que ce soit, des signaux acoustiques ne sera d'aucune utilité à un fraudeur pour se faire identifier par les services informatiques du prestataire de service. En effet, les signaux acoustiques d'identification varient à chaque opération. C'est-à-dire chaque fois que la carte est actionnée.

De préférence la dite carte comporte en outre :

- un compteur incrémental interconnecté aux moyens d'émission et aux moyens de cryptage s'incrémentant d'au moins une unité chaque fois que la carte est actionnée.

De sorte que l'état du compteur incrémental est émis à destination des moyens informatiques et que les signaux acoustiques sont cryptés en fonction de l'état du compteur incrémental.

De préférence également les dits moyens informatiques comportent en outre :

- des moyens de mémorisation de l'état C(p,m) du compteur incrémental lors de la dernière opération validée,

- des moyens de comparaison de l'état C(p,n) du compteur incrémental émis lors de l'opération en cours avec l'état C(p,m) du compteur incrémental mémorisé.

De sorte que la vérification de l'opération en cours est rejetée si C(p,n) est inférieur ou égal à C(p,m) et est poursuivie si C(p,n) est strictement supérieur à C(p,m).

De préférence également les dits moyens de traitement et les dits moyens de comparaison des signaux électroniques et des données d'identification contenues dans la base de données comportent des moyens permettant de recalculer les signaux électroniques en

fonction de l'état C(p,n) du compteur incrémental et des données d'identification puis de les comparer aux signaux électroniques transmis. De sorte qu'en cas de coïncidence, l'abonné peut être immédiatement mis en communication avec les services du prestataire de service.

Afin d'augmenter la sécurité du système, dans une variante de réalisation, le système comprend en outre des seconds moyens de comparaison d'un code confidentiel personnel à l'abonné contenu dans la base de données, à un code confidentiel émis par l'abonné. Ce code est émis au moyen d'un clavier associé au terminal multimédia et/ou à la carte et transmis aux moyens informatiques du prestataire de service, par le réseau informatique de communication.

Ainsi, le prestataire de service a l'assurance que l'appelant est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

Dans une autre variante de réalisation, afin également de renforcer la sécurité du système et d'éviter que l'abonné ne puisse contester la demande qu'il a adressée au prestataire de service, le système comporte :

- des moyens logiciels de validation des ordres donnés par l'abonné au prestataire de service, après détection d'un signal acoustique crypté émis par la carte actionnée par l'abonné,
- des moyens logiciels d'édition d'un accusé de réception des ordres donnés destiné à être adressé à l'abonné.

Grâce à ce système, l'abonné a validé, par une signature électronique, l'ordre qu'il a donné au prestataire de service.

Au moins trois variantes de réalisation permettent de transmettre les signaux acoustiques d'identification au service informatique du prestataire de service.

Selon la première variante les moyens informatiques, dépendants des services informatiques du prestataire de service, comprennent :

* des moyens de téléchargement d'un logiciel de conversion dans le terminal multimédia, le dit logiciel de conversion convertit, sous la forme d'une séquence de bits, les signaux acoustiques d'identification reçus par le microphone du terminal multimédia,

* des moyens d'émission d'un ordre de transmission de la séquence de bits, du terminal multimédia vers les services informatiques du prestataire de service, via le réseau informatique du type Internet.

De sorte que les signaux provenant du terminal multimédia se présentent sous la forme d'une séquence de bits.

Selon la deuxième variante de réalisation, le terminal multimédia comprend des moyens de transmission des signaux acoustiques d'identification reçus par le microphone du terminal multimédia, sous la forme d'un fichier son. Ce fichier son est transmis, via le réseau informatique du type Internet vers le service informatique du prestataire de service, notamment après réception d'un signal émis par les services informatiques du prestataire de service. Dans le cas de cette variante, le traitement du fichier son et sa transformation en une séquence de bits sont effectués par les services informatiques du prestataire de service.

Selon la troisième variante, le système comprend un logiciel de conversion destiné à être mis en oeuvre dans le terminal multimédia. Le logiciel de conversion transforme les signaux acoustiques, reçus et transmis par le microphone du terminal multimédia, en des séquences de bits transmissibles à distance au moyen du réseau informatique du type Internet.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description de variantes de réalisation de l'invention, données à titre d'exemple indicatif et non limitatif. Les figures représentent :

- figure 1 : une vue schématique en perspective du système et du procédé selon l'invention,
- figure 2 : la carte sous la forme de bloc diagramme,
- figure 3 : l'algorithme de vérification de l'authenticité du signal transmis.
- figure 4 : sous la forme de bloc diagramme, la première variante de réalisation, caractérisée en ce que les services informatiques du prestataire de service télécharge un logiciel de conversion dans le terminal multimédia,
- figure 5 : sous la forme de bloc diagramme, la dite deuxième variante de réalisation, caractérisée en ce que les services informatiques du prestataire de service reçoivent un

fichier son transmis par le terminal multimédia,

- figure 6 présente, sous la forme de bloc diagramme, la dite troisième variante de réalisation, caractérisée en ce que les services informatiques du prestataire de service reçoivent des bits générés par le terminal multimédia au moyen d'un logiciel spécifique.

On présente maintenant en relation avec la figure 1 le système et le procédé selon l'invention. Le système et le procédé selon l'invention permettent aux utilisateurs 11 du réseau informatique du type Internet 15 disposant de terminaux multimédia 16 comportant un microphone 17, d'accéder de manière sûre et rapide, aux services 30 que le prestataire de service 12 offre aux utilisateurs 11. Le terminal multimédia 16, situé à distance des services informatiques 18 du prestataire de service 12, est connecté au réseau informatique du type Internet 15.

Le système comprend une carte 10, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et pour chaque abonné 11. Cette carte est mise à la disposition des utilisateurs abonnés 11 par le prestataire de service 12 et ses services 40. La carte 10 comporte des moyens d'émission, notamment un haut parleur 13 émettant de brefs signaux acoustiques d'identification 20, de type DTMF. Ces signaux sont émis lorsque les moyens d'émission 13 et les organes qui les contrôlent sont actionnés par le client au moyen d'un bouton 14 accessible de l'extérieur de la carte (non visible sur la figure 1 car situé sur l'autre côté de la carte). Ces moyens d'émission 13 sont excités par un générateur de signaux DTMF 99, contrôlé par un microprocesseur 104 alimenté par une pile 106 et piloté par un résonateur 107. Le microprocesseur 104 contenu dans la carte comporte des moyens de cryptage 103 permettant de crypter, au moins en partie, les signaux acoustiques 20, comportant un algorithme de cryptage 108 et des identifiants 109 spécifiques pour chaque carte 10 et pour chaque abonné 11, notamment la clé secrète 250 utilisée par algorithme de cryptage 108.

Les signaux acoustiques 20 sont reçus par le microphone 17 du combiné téléphonique, contre lequel le client accole la carte 10. Le système comprend également des moyens de transmission 19 des signaux acoustiques 20, situés dans le terminal multimédia 16. Ces moyens de transmission 19 transmettent à distance les signaux acoustiques, après traitement et conversion en signaux électroniques, via le réseau informatique du type

Internet 15.

Le système comprend également des moyens informatiques 21, dépendants des services informatiques 18 du prestataire de service, connectés au réseau informatique du type Internet 15 et recevant les signaux provenant des terminaux multimédia 16.

Les moyens informatiques 21 comprennent :

* des moyens pour actionner 22 les moyens de transmission 19 des terminaux multimédia 16,

* une base de données 23 contenant les références des cartes et des abonnés et leurs données d'identification,

* des moyens de traitement 24 et des moyens de comparaison 25 des signaux électroniques et des données d'identification contenues dans la base de données 23,

* des données d'identification contenues dans la base de données 23 et des données caractéristiques des abonnés et des cartes.

De sorte qu'en cas de coïncidence les services 30 du prestataire de service 12 sont immédiatement accessibles aux abonnés.

De préférence, le microprocesseur 104 et les moyens de cryptage 103 sont conçus de telle sorte que le signal acoustique 20 varie à chaque opération. En effet, crypter un code d'identification c'est le transformer en une suite d'informations, incompréhensibles pour tout un chacun, et que seul le titulaire de la clef de cryptage, pourra décrypter. Mais cela n'empêche absolument pas la copie du code d'identification crypté, soit au cours de sa transmission acoustique (magnétophone), soit par piratage de la ligne téléphonique. Cette copie, utilisée indûment par un fraudeur, sera traitée par le système récepteur comme ayant toutes les caractéristiques de l'original, puis interprétée afin de vérifier les identifiants de la carte.

Le problème posé est donc le suivant : comment rendre impossible toute tentative de reproduction ? Il sera ci-après décrit différentes variantes de réalisation du moyen général qui permet de faire la distinction entre l'original et la copie, lors de l'analyse du signal crypté reçu par les moyens informatiques 21, en insérant un élément distinctif dans le signal 20 du type DTMF émis par la carte 10.

L'une de variantes consiste à utiliser une fonction dite d'horodatage (par exemple, ainsi

qu'elle a été décrite dans le brevet US n° 4 998 279). Cette fonction d'horodatage exploite le paramètre "temps" qui évolue en permanence. La "copie" se trouve ainsi en retard quand elle est émise. Une telle solution nécessite une synchronisation entre les moyens d'émission 13 et les moyens informatiques 21. Pour cela tous les deux doivent disposer d'une "base de temps" et d'un "étalon de fréquence". Ces deux bases de temps ont leur précision propre et leur dérive propre. Il en résulte qu'elles se désynchronisent lentement, mais progressivement. Pour remédier à cette difficulté technique, une certaine dérive est tolérée entre les bases de temps des moyens d'émission 13 et des moyens informatiques 21. Plus cette dérive est importante, plus l'incertitude augmente sur la "validité" de l'information reçue et plus augmente le risque de fraude. Ainsi si une dérive de une minute est tolérée, toute copie illicite de l'émission du signal crypté, et réutilisée frauduleusement dans les 30 secondes qui suivent, sera perçue comme valide par le système d'analyse des moyens informatiques 21.

Une autre variante consiste à utiliser des listes incrémentales (par exemple, ainsi qu'elle a été décrite dans le brevet US n° 4 928 098). Le dispositif d'émission et celui de réception possèdent la liste ordonnée des cryptages successifs du code d'identification ou bien disposent des algorithmes permettant de les établir au fur et à mesure. A un instant donné les moyens informatiques 21 sont en attente du résultat crypté C(n). S'ils reçoivent effectivement le message C(n), il valide l'opération. Mais les moyens informatiques 21 peuvent recevoir un message différent, en effet l'utilisateur de la carte peut avoir actionnée plusieurs fois les moyens d'émission 13 de celle-ci, par jeu, par maladresse, de sorte que la carte est dans la situation d'émettre le résultat crypté C(n+p) lors de sa prochaine utilisation avec les moyens informatiques 21. Si les moyens informatiques 21 reçoivent un message différent, ils cherchent en avant, dans la liste de résultats cryptés successifs, s'il existe un message C(n+p) identique à celui reçu. Pour lever l'ambiguïté "est-ce un message authentique émis par l'émetteur ?" ou "est-ce un message frauduleux ?", la solution consiste à demander ou à attendre l'émission du message suivant. Si celui-ci est alors identique à C(n+p+1), le système valide alors le message et se place dans l'attente de la prochaine émission, dans l'état C(n+p+2). Si celui-ci est différent, le message n'est pas validé et le système d'analyse reste en attente du message C(n). Une telle variante de

réalisation n'est pas très ergonomique puisqu'elle oblige le titulaire de la carte à actionner plusieurs fois celle-ci.

Selon une variante de réalisation préférentielle, pour distinguer le signal original de sa copie, le microprocesseur 104 embarqué dans la carte 10 comporte un compteur incrémental 105. A chaque usage de la carte, le compteur incrémental 105 s'incrémente d'une ou de plusieurs unités. Bien évidemment, telle une roue à cliquet, celui-ci ne peut revenir en arrière, il ne peut qu'avancer à chaque usage.

Dans le cas de cette variante de réalisation, l'état C(p,n) 242 du compteur 105 entre dans le calcul du message crypté 244 émis par les moyens d'émission 13. La partie codée S(p,n) 241 est calculée par l'algorithme 108 (dont l'algorithme équivalent 247 est mémorisé dans les moyens informatiques 21) au moyen de la clé secrète 250 spécifique à chaque carte et de l'état C(p,n) 242 du compteur 105. La carte 10 émet, en plus du numéro d'identification I(p) 240 de la carte et du code d'identification crypté S(p,n) 241, l'état C(p,n) 242 de son compteur incrémental 105 à chaque émission. Les moyens informatiques 21 mémorisent 230, dans la base de données 23, l'état C(p,n) 242 du compteur incrémental 105 lors de la dernière opération validée. Ainsi, à chaque réception de message 244, les moyens de comparaison 25 des moyens informatiques 21 peuvent comparer 245 l'information reçue relative à l'état C(p,n) 242 du compteur 105, à la précédente information reçue C(p,m) 246 et gardée en mémoire 230, 23.

a) - Si l'état C(p,n) 242 du compteur 105 (fig. 2) exprimé dans le message 244 est strictement supérieur ($n > m$) à celui C(p,m) 246 précédemment reçu, alors le message 244 est accepté et l'analyse se poursuit.

b)- Si l'état C(p,n) 242 du compteur 105 exprimé dans le message 244 est inférieur ou égal ($n \leq m$) à celui C(p,m) 246 précédemment reçu, alors le message est refusé. Le message reçu ne peut être qu'une copie antérieurement effectuée ou un leurre informatique.

Si les conditions définies au point a) ci-dessus sont réunies, les moyens informatiques 21 permettent de lire la partie fixe I(p) 240 et de rechercher dans leur propre base de données 23, 230 la clé secrète correspondante de la carte. Les moyens de calcul 239 des moyens de traitement 24 peuvent alors au moyen l'algorithme 247, de l'état du compteur C(p,n)

242 et de la clé secrète Clé(p) 250, procéder au calcul du code crypté attendu par les moyens informatiques 21. Le code crypté S'(p,n) 248 ainsi calculé est comparé 249 à celui effectivement reçu S(p,n) 241, par les moyens de comparaison 25. Ce procédé et ces moyens permettent donc de valider ou d'invalider le message 244, sans qu'il soit nécessaire à l'utilisateur de la carte d'actionner plusieurs fois celle-ci, comme cela est le cas dans la variante de réalisation ci-dessus décrite.

L'existence au sein de la carte 10 d'un compteur incrémental 105 permet, sans coût supplémentaire, de fixer, au moment de la programmation individuelle de la carte, le nombre maximum de fois où la carte peut être utilisée. Une fois ce maximum atteint, celle-ci n'émet plus de message cohérent et est donc refusée par les moyens informatiques 21.

La trame 244 émise contient, pour une carte donnée (p),

- une partie fixe I(p) 240 (le numéro d'identification de la carte),
- une partie variable incrémentale C(p,n) 242 (l'état du compteur),
- une partie variable S(p,n) 241 apparemment aléatoire (le résultat d'un algorithme de cryptage 108 sur la clé secrète 250 propre à cette carte (p))

La trame émise

- est toujours différente d'une carte à l'autre,
- est, pour une carte donnée, toujours différente à chaque émission.

Les moyens informatiques 21 permettent, pour une carte donnée (p), de :

- lire la partie fixe I(p) 240 (le numéro d'identification de la carte),
- rechercher dans leur propre base de données 23 la clé secrète 250 de cette carte et le dernier enregistrement reçu de l'état C(p,m) 246 du compteur 105 de cette carte,
- rejeter cette trame 244 si l'état du compteur C(p,n) 242 de l'opération en cours est inférieur ou égal à celui C(p,m) 246 précédemment reçu et de poursuivre la vérification de l'opération en cours si l'état C(p,n) 242 est strictement supérieur à celui C(p,m) 246 précédemment reçu,
- de "décrypter" le message 244 reçu et d'en valider le contenu, en le recalculant au moyen de l'algorithme de cryptage 247, de la clé spécifique 250 de cette carte et de l'état du compteur C(p,n) 242, puis en comparant le résultat de ce calcul au message reçu.

Ainsi, grâce à cette combinaison de moyens il est possible d'émettre, au moyen d'une carte ayant le format d'une carte de crédit, des fréquences acoustiques de type DTMF d'identification, recevables par le microphone d'un équipement relié au réseau téléphonique, et d'avoir la certitude de l'authenticité de la carte appelante et d'écarter ainsi tous les fraudeurs utilisant tout enregistrement sonore ou informatique ou tout leurre informatique.

Afin d'augmenter la sécurité du système, dans la variante de réalisation représentée sur la figure 1, le système comprend en outre des seconds moyens de comparaison 26. Ces moyens de comparaison permettent de comparer un code confidentiel personnel à l'abonné contenu dans la base de données avec le code confidentiel émis par l'abonné. Ce code est émis au moyen d'un clavier 27 associé au terminal multimédia 16 et/ou à la carte 10 et transmis aux moyens informatiques du prestataire de service, par le réseau informatique de communication 15.

Ainsi, le prestataire de service a l'assurance que l'appelant 11 est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

Afin également de renforcer la sécurité du système et d'éviter que l'abonné ne puisse contester la demande qu'il a adressée au prestataire de service, les moyens informatiques 21 (dans la variante de réalisation représentée sur la figure 1) comprennent :

- des moyens logiciels de validation 21a des ordres donnés par l'abonné au prestataire de service, après détection d'un signal acoustique crypté émis par la carte actionnée par l'abonné,
- des moyens logiciels d'édition 21b d'un accusé de réception des ordres donnés destiné à être adressé à l'abonné.

Grâce à ce système, l'abonné a validé, par une signature électronique, l'ordre qu'il a donné au prestataire de service.

En se référant aux figures 4, 5 et 6, on va maintenant décrire trois variantes de réalisation qui permettent de transmettre les signaux acoustiques d'identification 20 au service informatique 18 du prestataire de service 12. On a utilisé les mêmes références sur ces figures pour désigner les organes et les moyens qui ont été décrits en rapport avec la

figure 1.

Selon la première variante de réalisation (figure 4), les moyens informatiques 21, dépendants des services informatiques 18 du prestataire de service, comprennent des moyens de téléchargement 200 dans le terminal multimédia 16, d'un logiciel de conversion du fichier son en bits. De sorte que les signaux provenant du terminal multimédia 16 se présentent sous la forme d'une séquence de bits.

Selon la deuxième variante (figure 5), le terminal multimédia 16 comprend des moyens de conversion et de transmission 300 des signaux acoustiques d'identification reçus par le microphone du terminal multimédia, sous la forme d'un fichier son. Ce fichier son est transmis notamment après réception d'un signal émis par les services informatiques 18 du prestataire de service. Ce signal est émis après que la connexion téléphonique ait été établie entre le terminal et le service informatique. Dans le cas de cette variante le traitement du fichier son et sa transformation en une séquence de bits sont effectués par les moyens informatiques 21 des services informatiques 18 du prestataire de service.

Selon la troisième variante (figure 6), le prestataire de service fournit à l'abonné un logiciel de conversion (400) que celui-ci entre dans son terminal multimédia 16. Ce logiciel de conversion transforme les signaux acoustiques reçus et transmis par le microphone 17 du terminal multimédia 16, en des signaux numériques transmissibles à distance au moyen du réseau informatique du type Internet 15.

REVENDICATIONS

1. Procédé permettant aux utilisateurs (11) d'un réseau informatique du type Internet, disposant de terminaux multimédia (16) comportant un microphone (17) et connectés au réseau informatique du type Internet, situés à distance d'un prestataire de service (12), d'accéder de manière sûre et rapide, aux services (30) que ce prestataire de service (12) offre aux utilisateurs (11) du réseau informatique du type Internet,
le dit procédé comprenant les étapes suivantes :

- le prestataire de service (12) met à la disposition de chacun des utilisateurs (11) du réseau informatique du type Internet qui se sont abonnés à ses services une carte (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque abonné et pour chaque carte, la dite carte (10), au format carte de crédit, émet de brefs signaux acoustiques d'identification (20), de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée (14) par l'utilisateur (11) du réseau informatique du type Internet,
- les dits signaux acoustiques d'identification (20) sont reçus par le microphone (17) du terminal multimédia (16) et transmis via le réseau informatique (15) du type Internet au service informatique (18) du prestataire de service,
- les signaux transmis et les données d'identification de l'abonné et de la carte détenues (23) par le service informatique (18), sont traités (24) et comparés (25) électroniquement par le service informatique (18) du prestataire de service,

de sorte qu'en cas de coïncidence, l'abonné (11) peut être immédiatement mis en communication avec les services (30) du prestataire de service (12).

2. Procédé selon la revendication 1,
- la dite carte (10) :
  * décompte (105) en outre le nombre de fois C(p,n) (242) où elle est actionnée par l'élément (14),
  * émet des signaux acoustiques (20) représentatifs du nombre de fois C(p,n) (242) où elle a été actionnée,
  * crypte (103) les signaux acoustiques en fonction du nombre de fois C(p,n) (242) où elle a été actionnée,

- les moyens informatiques (21) du service informatique (18) traitant (24) et comparant (25) électroniquement les signaux transmis et les données d'identification du client et de la carte détenues (23) par le service informatique (18) du prestataire de service :

* mémorisent (230) le nombre de fois C(p,m) (246) où la carte a été actionnée lors de dernière opération validée,

* comparent (245) le nombre de fois C(p,n) (242) où la carte a été actionnée, lors de l'opération en cours, avec le nombre de fois mémorisé C(p,m) (246),

* rejettent l'opération en cours si C(p,n) (242) est inférieur ou égal à C(p,m) (246) et poursuivent la vérification de l'opération en cours si C(p,n) (242) est supérieur à C(p,m) (246),

* recalculent (239) les signaux électroniques S'(p,n) (248) en fonction des données d'identification et du nombre de fois C(p,n) (242) où la carte a été actionnée, lors de l'opération en cours, puis les comparent (249) aux signaux électroniques transmis S(p,n) (241).

de sorte qu'en cas de coïncidence, l'abonné (11) peut être immédiatement mis en communication avec les services (30) du prestataire de service (12).

3. Procédé selon les revendications 1 ou 2, comprenant en outre l'étape suivante :

- l'abonné (11) émet, au moyen d'un clavier (27) associé au terminal multimédia (16) et/ou à la carte (10), un code confidentiel, après transmission au service informatique (18) du prestataire de service (12), via le réseau informatique (15) du type Internet, ce code confidentiel est traité et comparé au code confidentiel personnel de l'abonné détenu (23) par le service informatique (18) du prestataire de service (12).

4. Procédé selon les revendications 1, 2 ou 3, comprenant en outre l'étape suivante :

- les ordres donnés par l'abonné (11) aux services (30) du prestataire de service (12) sont validés par l'abonné en actionnant la carte (10) pour qu'elle émette un signal acoustique crypté de validation,

- le dit signal de validation est enregistré par le service informatique (18) du prestataire de service (12),

de sorte que l'abonné (11) a validé, par une signature électronique, l'ordre qu'il a donné au prestataire de service (12).

5. Procédé selon les revendications 1, 2, 3 ou 4, comprenant en outre les étapes suivantes :

- les signaux acoustiques d'identification (20), reçus par le microphone (17) du terminal multimédia (16) et transmis via le réseau informatique (15) du type Internet au service informatique (18) du prestataire de service (12), sont transmis sous la forme d'un fichier son.

6. Procédé selon les revendications 1, 2, 3 ou 4, comprenant en outre les étapes suivantes :

- le service informatique (18) du prestataire de service (12) télécharge dans le terminal multimédia un logiciel de conversion,
- le logiciel de conversion convertit sous la forme d'une séquence de bits les signaux acoustiques d'identification (20) reçus par le microphone (17) du terminal multimédia (16),
- la séquence de bits est transmise, via le réseau informatique (15) du type Internet, au service informatique (18) du prestataire de service (12),

de sorte que les signaux provenant du terminal multimédia se présentent sous la forme d'une séquence de bits.

7. Procédé selon les revendications 1, 2, 3 ou 4, comprenant en outre les étapes suivantes :

- le prestataire de service (12) met à la disposition de chacun des utilisateurs (11) du réseau informatique (15) du type Internet qui se sont abonnés à ses services (30), un logiciel de conversion destiné à être mis en oeuvre dans le terminal multimédia (16),
- les dits signaux acoustiques d'identification (20) reçus par le microphone (17) du terminal multimédia (16) sont convertis en séquence de bits, avant d'être transmis via le réseau informatique (15) du type Internet au service informatique (18) du prestataire de service.

8. Système permettant aux utilisateurs du réseau informatique (15) du type Internet disposant de terminaux multimédia (16) comportant un microphone (17), connectés au réseau informatique du type Internet, situés à distance d'un prestataire de service (12), d'accéder de manière sûre et rapide, aux services (30) que le dit prestataire de service (12)

offre aux utilisateurs abonnés (11),

le dit système comprenant :

- une carte (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et pour chaque abonné, mise à la disposition de ceux-ci, la dite carte (10) comportant :

  * des moyens d'émission (13) de brefs signaux d'identification (20), de type DTMF, actionnés par l'abonné au moyen d'un élément (14) accessible de l'extérieur de la carte (10),

  * des moyens de cryptage (103) permettant de crypter au moins en partie et de varier les signaux acoustiques (20) chaque fois que la carte (10) est actionnée (14),

- des moyens de transmission (19) des signaux acoustiques (20), situés dans les terminaux multimédia (16), transmettant à distance sous la forme de signaux électroniques, via le réseau informatique (15) du type Internet, les dits signaux acoustiques (20),

- des moyens informatiques (21), dépendants des services informatiques (18) du prestataire de service (12), connectés au réseau informatique (15) du type Internet et recevant les signaux provenant des terminaux multimédia (16), les dits moyens informatiques (21) comprenant :

  * une base de données (23) contenant les références des cartes (10) et des abonnés (11) et leurs données d'identification,

  * des moyens de traitement (24) et des moyens de comparaison (25) des signaux électroniques et des données d'identification contenues dans la base de données (23),

de sorte qu'en cas de coïncidence les services (30) du prestataire de service (12) sont immédiatement accessibles aux abonnés (11).

9. Système selon la revendications 8,

- la dite carte (10) comportant en outre :

  * un compteur incrémental (105) interconnecté aux moyens d'émission (13) et aux moyens de cryptage (103), s'incrémentant d'au moins une unité chaque fois que la carte (10) est actionnée par l'élément (14),

de sorte que l'état du compteur incrémental (105) est émis à destination des moyens

informatiques (21) et que les signaux acoustiques sont cryptés en fonction de l'état du compteur incrémental,

- les dits moyens informatiques (21) comportant en outre :

* des moyens de mémorisation (23, 230) de l'état C(p,m) (246) du compteur incrémental (105) lors de la dernière opération validée,

* des moyens de comparaison (245) de l'état C(p,n) (242) du compteur incrémental (105) émis lors de l'opération en cours avec l'état C(p,m) (246) du compteur incrémental mémorisé,

de sorte que la vérification de l'opération en cours est rejetée si C(p,n) (242) est inférieur ou égal à C(p,m) (246) et est poursuivie si C(p,n) (242) est strictement supérieur à C(p,m) (246),

- les dits moyens de traitement (24) et les dits moyens de comparaison (25) des signaux électroniques et des données d'identification contenues dans la base de données comportant des moyens permettant de recalculer (239) les signaux électroniques en fonction de l'état C(p,n) (242) du compteur incrémental (105) et des données d'identification puis de les comparer (249) aux signaux électroniques transmis,

de sorte qu'en cas de coïncidence les services (30) du prestataire de service (12) sont immédiatement accessibles aux abonnés (11).

10. Système selon les revendications 8 ou 9, les dits moyens informatiques (21) comprenant en outre:

- des seconds moyens de comparaison (26) d'un code confidentiel personnel à l'abonné contenu dans la base de données (23), à un code confidentiel émis par l'abonné au moyen d'un clavier (27) associé au terminal multimédia (16) et/ou à la carte (10) et transmis aux moyens informatiques (21) du prestataire de service (12), par le réseau informatique de communication (15).

11. Système selon les revendications 8, 9, ou 10, les dits moyens informatiques (21) comprenant en outre :

- des moyens logiciels de validation (21a) des ordres donnés par l'abonné (11) au prestataire de service (12), après détection d'un signal acoustique crypté émis par la carte (10) actionnée par l'abonné,

- des moyens logiciels d'édition (21b) d'un accusé de réception des ordres donnés destiné à être adressé à l'abonné.

12. Système selon les revendications 8, 9, 10 ou 11,

- le terminal multimédia comprenant des moyens de transmission (300) des signaux acoustiques d'identification (20) reçus par le microphone (17) du terminal multimédia (16), sous la forme d'un fichier son, via le réseau informatique (15) du type Internet, vers le service informatique (18) du prestataire de service (12).

13. Système selon les revendication 8, 9, 10 ou 11 :

- les moyens informatiques (21), dépendants des services informatiques (18) du prestataire de service (12), comprenant :

  * des moyens de téléchargement (200) d'un logiciel de conversion dans le terminal multimédia (16), le dit logiciel de conversion convertissant, sous la forme d'une séquence de bits, les signaux acoustiques d'identification (20) reçus par le microphone (17) du terminal multimédia (16),

  * des moyens d'émission d'un ordre de transmission de la séquence de bits, du terminal multimédia (16) vers les services informatiques (18) du prestataire de service, via le réseau informatique (15) du type Internet,

de sorte que les signaux provenant du terminal multimédia se présentent sous la forme d'une séquence de bits.

14. Système selon les revendications 8, 9, 10 ou 11, comprenant :

- un logiciel de conversion destiné à être mis en oeuvre dans le terminal multimédia (16), le dit logiciel de conversion transformant les signaux acoustiques (20) reçus et transmis par le microphone (17) du terminal multimédia, en des signaux numériques transmissibles à distance via le réseau informatique (15) du type Internet.

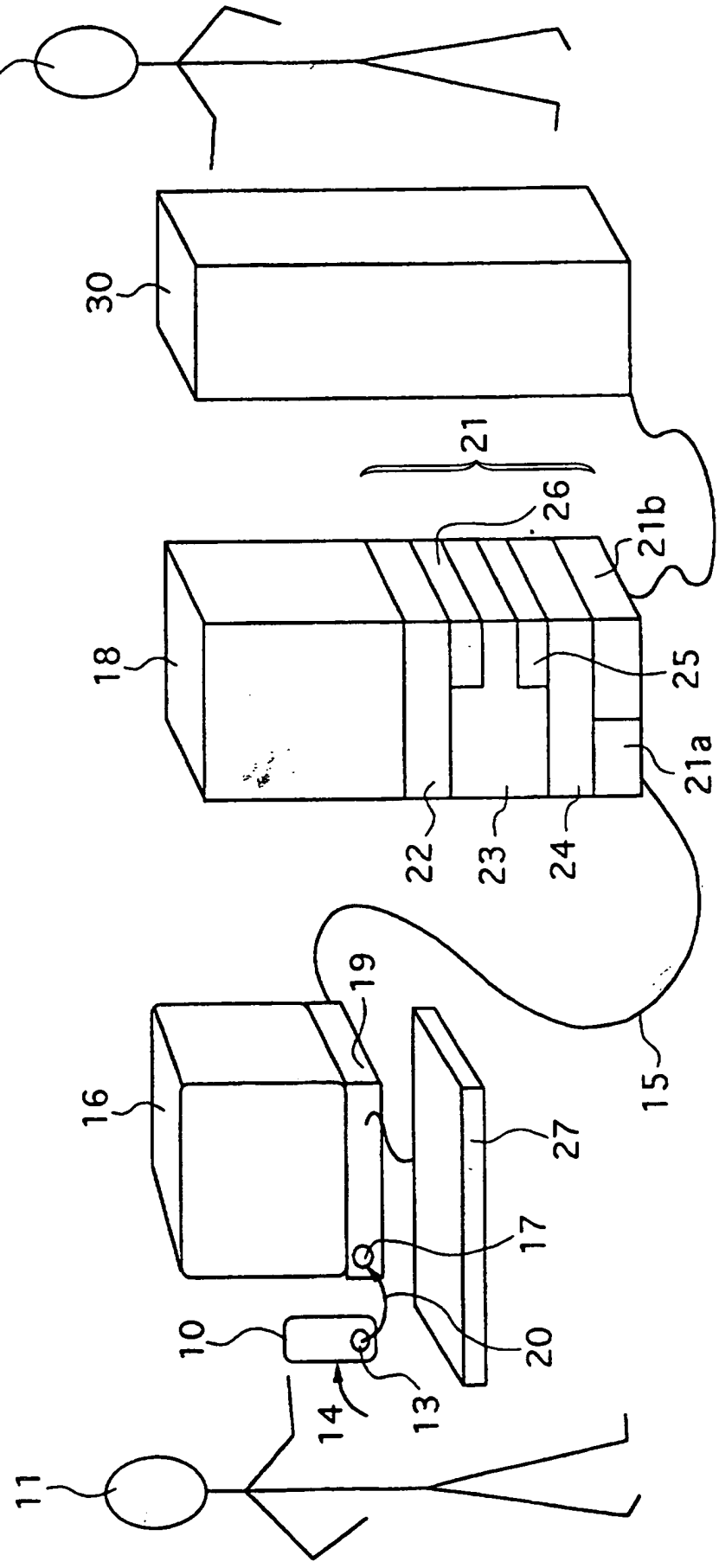


Fig. 1

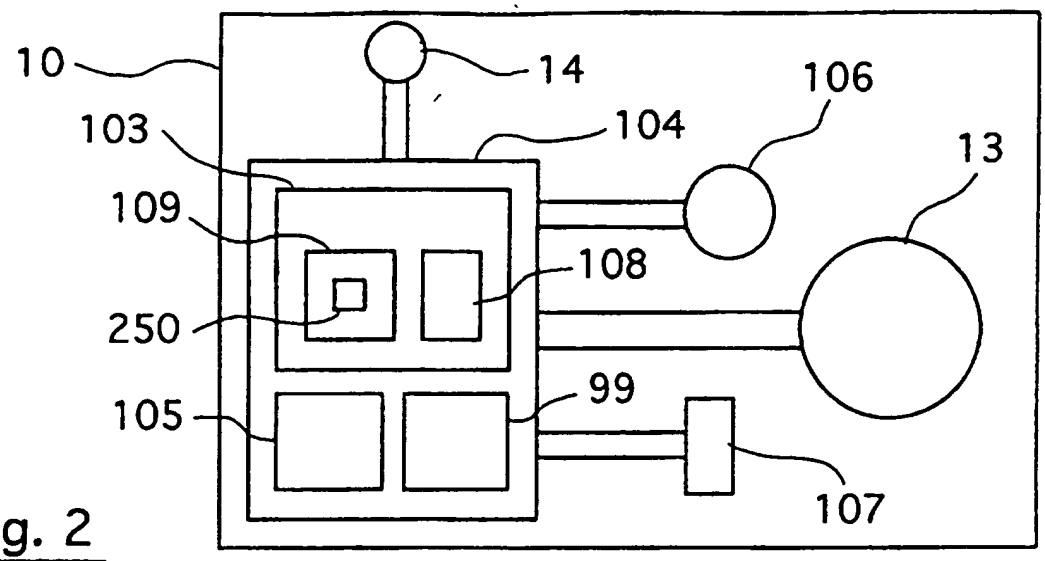

10
14
106
103
104
13
109
108
250
99
105
107

Fig. 2

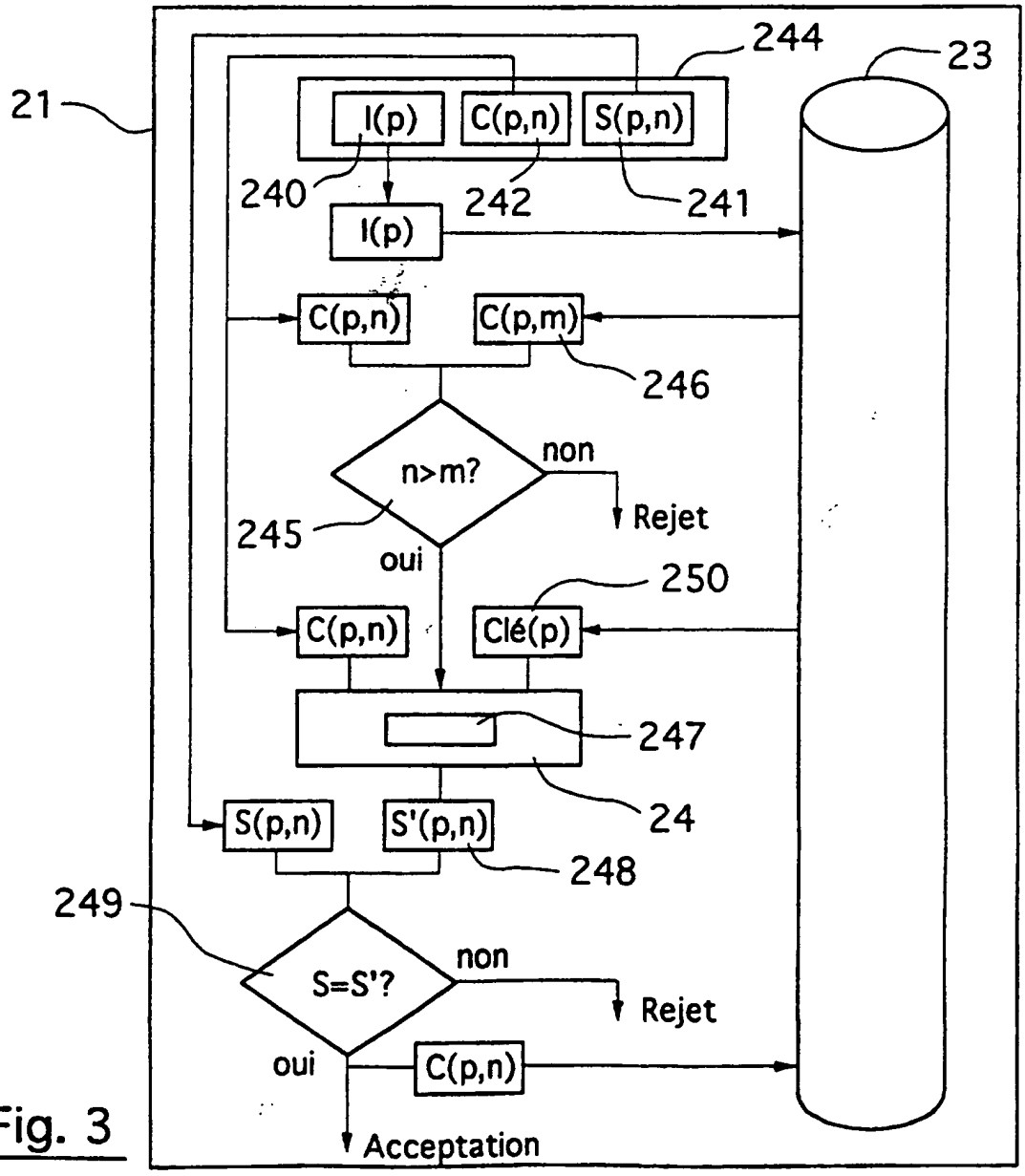

244
23
21
I(p)
C(p,n)
S(p,n)
240
242
241
I(p)
C(p,n)
C(p,m)
246
n>m?
non
Rejet
245
oui
250
C(p,n)
Clé(p)
247
24
S(p,n)
S'(p,n)
248
249
S=S'?
non
Rejet
oui
C(p,n)
Acceptation

Fig. 3

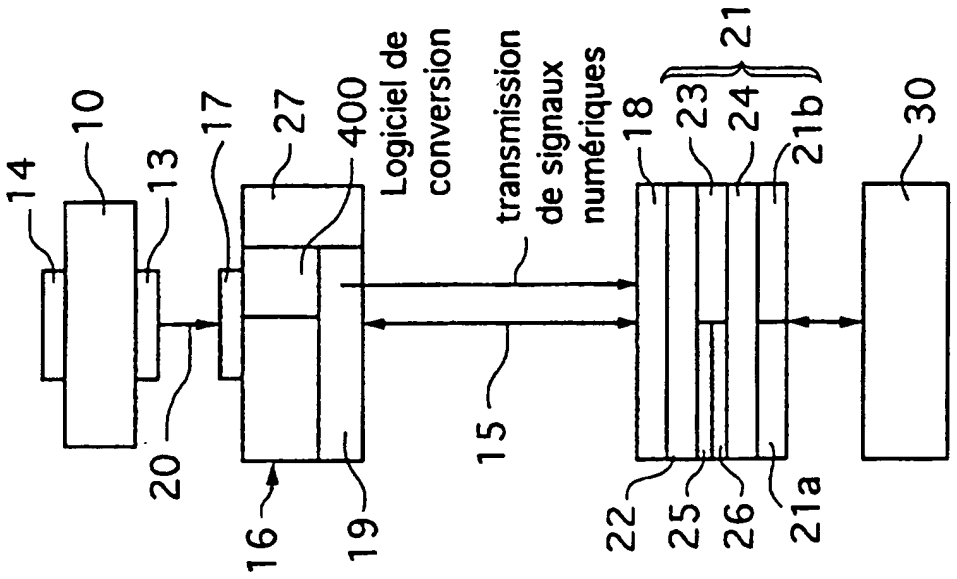


Fig. 6

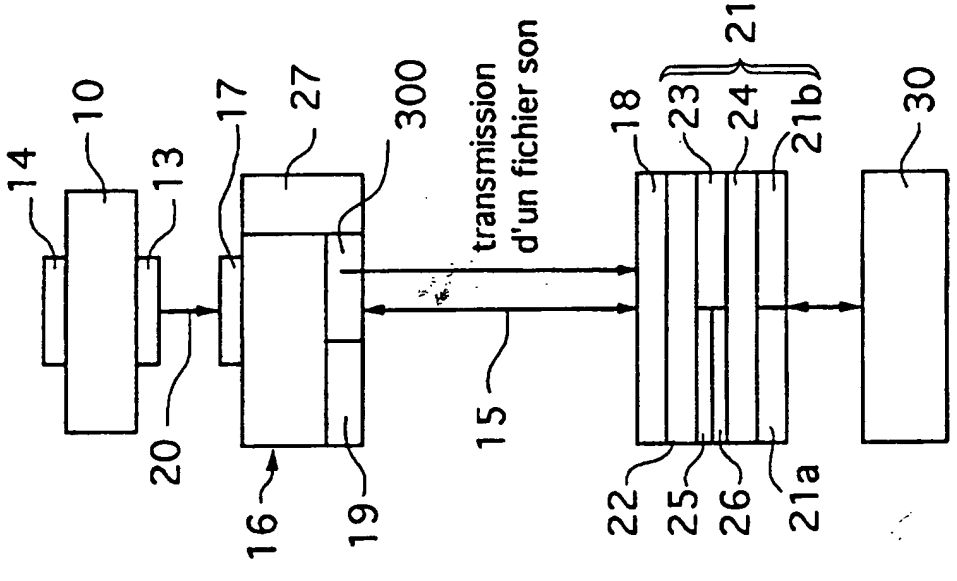


Fig. 5

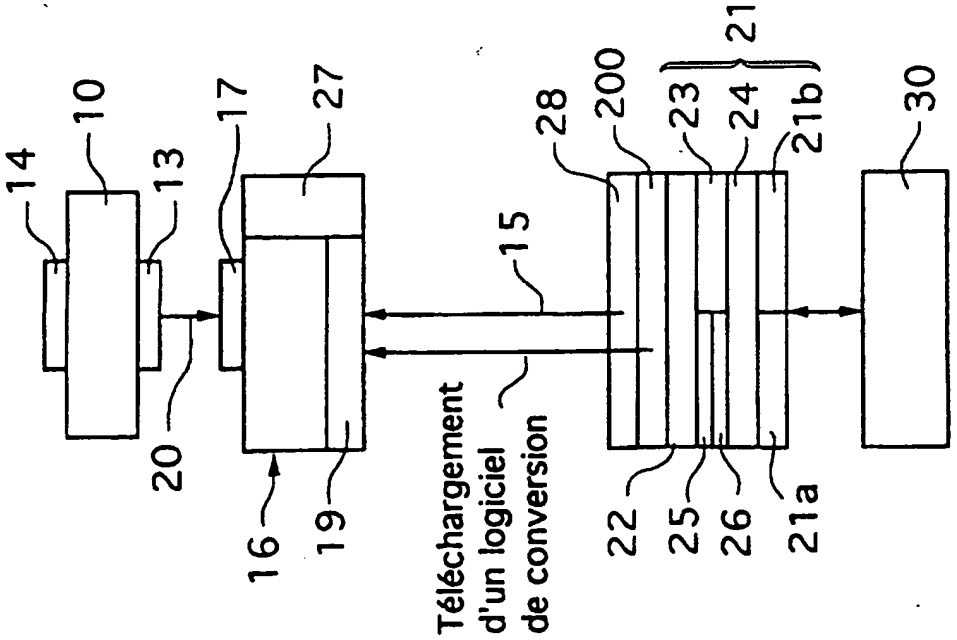


Fig. 4

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/FR 97/01685

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04M1/274 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04M G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 374 012 A (ETAT FRANCAIS) 20 June 1990 see column 1, line 1 - line 54 see column 4, line 25 - line 49 ---	1,8
A	CA 2 085 775 A (BOURRE MICHEL ;LAZZARINI GABRIEL (CA); TROLI JOHN (CA)) 19 June 1994 see the whole document ---	1,8
A	GB 2 274 523 A (PATNI) 27 July 1994 see abstract see page 2, line 16 - last line --- -/--	1,8

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 February 1998	18/02/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

INTERNATIONAL SEARCH REPORT

Intern. al Application No
PCT/FR 97/01685

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 459 781 A (NANOTEQ) 4 December 1991 see column 3, line 56 - column 4, line 28 see column 5, line 20 - line 26 see column 7, line 42 - line 52 see column 9, line 48 - line 50 see column 11, line 35 - line 45 -----	2,9

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern .al Application No
PCT/FR 97/01685

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 374012 A	20-06-90	FR 2640835 A	22-06-90
CA 2085775 A	19-06-94	NONE	
GB 2274523 A	27-07-94	NONE	
EP 459781 A	04-12-91	AT 136975 T	15-05-96
		DE 69118748 D	23-05-96
		DE 69118748 T	28-11-96
		ES 2085425 T	01-06-96
		US 5517187 A	14-05-96

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 97/01685

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04M1/274 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 H04M G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 374 012 A (ETAT FRANCAIS) 20 juin 1990 voir colonne 1, ligne 1 - ligne 54 voir colonne 4, ligne 25 - ligne 49 ---	1,8
A	CA 2 085 775 A (BOURRE MICHEL ;LAZZARINI GABRIEL (CA); TROLI JOHN (CA)) 19 juin 1994 voir le document en entier ---	1,8
A	GB 2 274 523 A (PATNI) 27 juillet 1994 voir abrégé voir page 2, ligne 16 - dernière ligne --- -/--	1,8

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités

"A" document définissant l'état général de la technique non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
9 février 1998	18/02/1998

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 97/01685

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 459 781 A (NANOTEQ) 4 décembre 1991 voir colonne 3, ligne 56 - colonne 4, ligne 28 voir colonne 5, ligne 20 - ligne 26 voir colonne 7, ligne 42 - ligne 52 voir colonne 9, ligne 48 - ligne 50 voir colonne 11, ligne 35 - ligne 45	2,9

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 97/01685

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 374012 A	20-06-90	FR 2640835 A	22-06-90
CA 2085775 A	19-06-94	AUCUN	
GB 2274523 A	27-07-94	AUCUN	
EP 459781 A	04-12-91	AT 136975 T	15-05-96
		DE 69118748 D	23-05-96
		DE 69118748 T	28-11-96
		ES 2085425 T	01-06-96
		US 5517187 A	14-05-96